

Hoe werken **spamfilters?**

Ook jij krijgt waarschijnlijk spam: het begint onschuldig met enkele berichtjes, maar soms ontvang je er wel honderd per dag. Wat is spam of junk e-mail eigenlijk? En hoe werken spamfilters op de servers van je provider én op je computer? Clickx ploos het voor je uit... FREDERICK GORDTS

Volgens de Messaging Anti-Abuse Working Group www.maawg.com is 85% van alle e-mail spam, of zo'n 55 miljoen berichten per dag. En dat kan wel eens kloppen, want ook onze mailbox puilt uit van de spam. Spam is het misbruiken van e-mailservers om op die manier ongewenste e-mails te versturen naar willekeurige e-mailadressen. Vaak betreft het commerciële berichten die je willen aanzetten om bepaalde producten te kopen of websites te bezoeken.

Waarom?

Je vraagt je waarschijnlijk af waarom je zoveel spam krijgt: per slot van rekening verwijder je die spamberichten onmiddellijk en komt het waarschijnlijk nooit in je op om op zo'n dubieus commercieel aanbod in te gaan. Dat denkt ook de overgrote meerderheid van de bevolking, maar helaas niet iedereen. Spammers sturen vaak miljoenen keer hetzelfde berichtje door. De reden: het kost hen niets, want bandbreedte is vaak onbeperkt (bijvoorbeeld met een breedband-abonnement of via een server met honderden gigabytes of terabytes inbegrepen bandbreedte). Als op 0,000001% van de berichten een positief resultaat (een antwoord) komt, is het voor de spammer al een succes en verkoopt hij al snel tientallen of honderden "producten". En lukt het niet, dan probeert hij het gewoon nog eens.

Waarom ik?

Je opent een e-mailaccount en binnen enkele uren ontvang je al spam? Dat is "normaal", en je kan er niets aan doen: spammers struinen namelijk het internet af naar adressen (op websites en nieuwsgroepen), maar versturen ook vaak naar willekeurige adressen, zoals FRANK@MIJNDOMEIN.BE. Ze proberen gewoon vaak voorkomende gebruikersnamen of laten een woordgenerator los op de adressen. Foutmeldingen van onbestaande adressen worden verder gewoon genegeerd.

Mag het wel?

Spam versturen mag niet. Het mag niet van de internetprovider(s) die de spammer gebruikt, en mails versturen zonder toestemming van de ontvanger mag ook niet van de Europese Unie. Ook in andere regio's, zoals de VS en Australië, is spammen verboden...

Spamfilters

Hoewel spammen niet mag, kan je er weinig aan doen. Je kan om de week of om de maand van e-mailadres veranderen, maar dat zullen je kennissen, vrienden of collega's niet leuk vinden, en ook voor jou is het niet handig om steeds opnieuw je e-mailprogramma te configureren. Je kan de spammer voor de rechter slepen, maar vaak weet je niet eens wie de spammer is... De enige haalbare oplossing is gebruik maken van spamfilters. Een spamfilter, of e-mailfilter, zorgt ervoor dat bepaalde berichten, die er uitzien als spam, verwijderd worden. Er bestaan twee soorten spamfilters:

- Spamfilters op de e-mailserver van je provider
- Spamfilters op jouw computer

Idealiter gebruik je een combinatie van beide. Hieronder leggen we uit hoe beide soorten spamfilters werken:

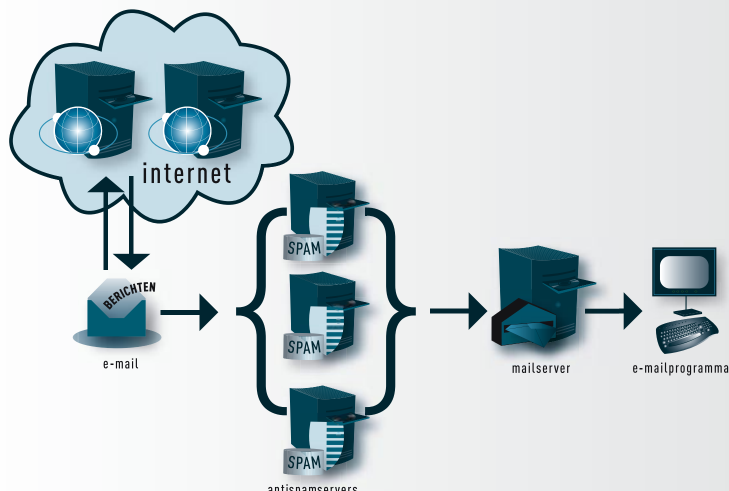
1. SPAMFILTERS BIJ JE PROVIDER

Elke e-mail die naar jou gestuurd wordt, belandt eerst op de e-mailserver van je provider. Deze server, ook wel de mailserver, POP- of POP3-server genaamd, bewaart alle e-mail tot jij, met je e-mailprogramma, je mail controleert of "checkt". De mailserver van je provider geeft dan door hoeveel berichten er zijn, waarna je e-mailprogramma die berichten binnenhaalt. Daarna worden de berichten van de server verwijderd, zodat er plaats gemaakt wordt voor nieuwe.

Voor binnenkomende berichten op de mailserver van je provider kan een spamfilter geactiveerd worden, eventueel op een aparte server. Die spamfilter geeft aan elk bericht een bepaalde "score" om te bepalen of het bericht spam is. Is het bericht spam, dan wordt het vaak meteen verwijderd. Soms wordt ook de vermelding [SPAM] aan het onderwerp van het bericht toegevoegd, zodat je snel kan zien dat het om spam gaat. Je kan het bericht dan alsnog lezen, of het meteen (laten) verwijderen door een e-mailfilter of -regel in je mailprogramma te configureren. Bij heel wat providers kan je de spamfilter op de mailserver configureren. Dat kan via een speciale pagina, of via de webmailsite van je provider. Je kan er niet alleen bepalen hoe "streng" de filter moet zijn, maar ook of bepaalde adressen op een white- of blacklist moeten komen. Aan een whitelist voeg je adressen (of zelfs domeinnamen) toe van mensen waarvan je zeker weet dat ze nooit spam versturen; vrienden dus. Dergelijke berichten worden dan nooit als spam



SPAMFILTERS



gemarkeerd. Krijg je echter soms spam die niet als dusdanig gemarkeerd wordt, dan kan je het e-mailadres van de spammer toevoegen aan de blacklist. Het resultaat is dat zijn mails meteen als spam gemarkeerd worden. Maar let op: veel spammers veranderen voor elk bericht van e-mailadres, zodat dit vaak geen zin heeft.

2. SPAMFILTERS OP JE COMPUTER

Biedt je provider geen spamfilter aan op de server, of blijf je toch nog spam ontvangen, dan kan je ook op je eigen computer een spamfilter installeren. Dat is vaak een stukje software zoals Spamfighter www.spamfighter.com. Gebruik je bepaalde software, zoals Outlook 2003, dan is er misschien al een spamfilter ingebouwd. Net als een antivirusprogramma moet je een spamfilter regelmatig updaten. Een update bevat vaak lijsten van "nieuwe" spammers, maar ook nieuwe soorten berichten, zodat de filters efficiënter werken. Sommige software, zoals Cloudmark Desktop www.cloudmark.com/desktop/download, gaat nog een stapje verder en gebruikt een eigen netwerk van servers dat continu de laatste spamberichten en -plagen in het oog houdt. Je moet zo'n software dus niet zelf updaten; dat gebeurt automatisch en vaak meerdere keren per dag. Bij Cloudmark mogen gebruikers trouwens ook zelf aangeven dat bepaalde berichten spam zijn, zodat nieuwe spamberichten nog sneller gewist worden. Nadeel van dergelijke software is dat je wel een maandelijks of jaarlijks abonnement moet aangaan, bijvoorbeeld € 35 per jaar voor Cloudmark Desktop.

Hoe werkt een spamfilter?

Technisch is een spamfilter erg complex, maar het is gebaseerd op kansberekening en regels of "rules". Aan elk mailtje wordt door een spamfilter een score gegeven, tussen 0 en 100. Een spamfilter bevat onder andere lijsten met "verdachte" woorden. Staan er meerdere verdachte woorden in een mailtje, dan is de kans groter dat dit mailtje spam is, en gaat de score omhoog. Verder wordt ook nog gecontroleerd of er wel een afzender is vermeld, en of de naam van die afzender ook vermeld wordt. Spamfilters kijken ook na of een mailtje in html of "rich text" verstuurd werd. Is dat zo, dan is de kans groter dat een mailtje spam is. Ook als er heel wat "lege" regels in een mailtje staan, stijgt de kans dat het om spam gaat. Zo zijn er duizenden regels; kijk maar eens bij SpamAssassin http://spamassassin.apache.org/tests_3_1_x.html, een spamfilter voor servers. ♦